AnyConnect 및 ISE 서버로 SD-WAN 원격 액세스 (SDRA) 구성

목차

소개

이 문서에서는 CA 서버로 Cisco IOS® XE 자동 모드를 사용하여 AnyConnect 클라이언트를 사용하여 SD-WAN SDRA(Remote Access)를 구성하는 방법과 인증, 권한 부여 및 계정 관리를 위해 Cisco ISE(Identity Services Engine) 서버를 구성하는 방법에 대해 설명합니다.

사전 요구 사항

요구 사항

다음 주제에 대한 지식을 보유하고 있으면 유용합니다.

- Cisco SD-WAN(Software-defined Wide Area Network)
- PKI(Public Key Infrastructure)
- FlexVPN
- RADIUS 서버

사용되는 구성 요소

이 문서의 정보는 다음 소프트웨어 및 하드웨어 버전을 기반으로 합니다.

- C8000V 버전17.07.01a
- vManage 버전 20.7.1
- CSR1000V 버전 17.03.04.a
- ISE 버전 2.7.0.256
- AnyConnect Secure Mobility Client 버전 4.10.04071

이 문서의 정보는 특정 랩 환경의 디바이스를 토대로 작성되었습니다. 이 문서에 사용된 모든 디바이스는 초기화된(기본) 컨피그레이션으로 시작되었습니다. 네트워크가 작동 중인 경우 모든 명령의 잠재적인 영향을 이해해야 합니다.

배경 정보

원격 액세스 VPN이란?

원격 액세스 VPN을 사용하면 원격 사용자가 회사 네트워크에 안전하게 연결하고 애플리케이션 및 사무실에 연결된 장치만 액세스할 수 있는 데이터를 사용할 수 있습니다.

원격 액세스 VPN은 직원의 디바이스와 회사 네트워크 간에 생성된 가상 터널을 통해 작동합니다.

이 터널은 공용 인터넷을 통과하지만, 이를 통해 송수신되는 데이터는 암호화 및 보안 프로토콜로 보호되어 안전하게 보관됩니다.

이 VPN 유형의 두 가지 주요 구성 요소는 네트워크 액세스 서버/RA 헤드엔드 및 VPN 클라이언트 소프트웨어입니다.

SD-WAN 원격 액세스 VPN이란 무엇입니까?

Remote Access는 별도의 Cisco SD-WAN 및 RA 인프라를 필요로 하지 않고 Cisco AnyConnect를 RA 소프트웨어 클라이언트로 사용하여 RA 서비스를 신속하게 확장할 수 있도록 SD-WAN 솔루션에 통합되었습니다.

원격 액세스는 원격 사용자가 조직의 네트워크에 액세스할 수 있도록 합니다. 이렇게 하면 재택 작업이 가능합니다.

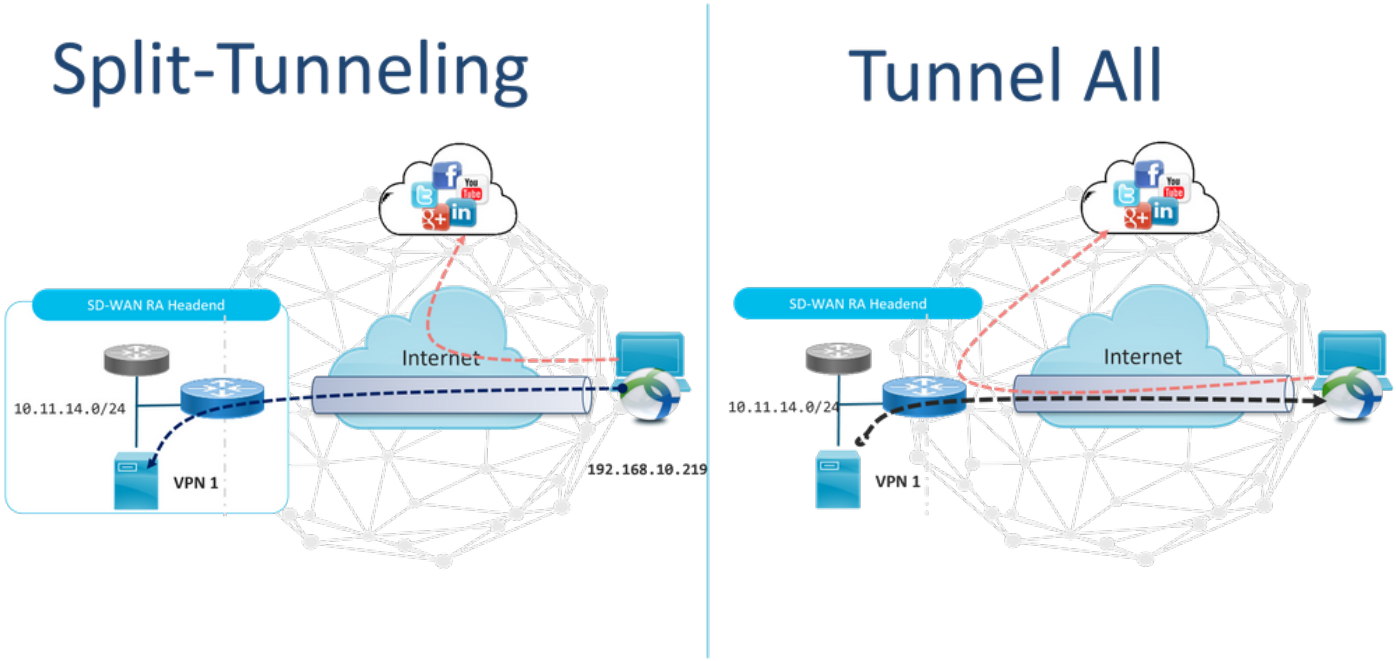
장점

- RA는 원격 위치의 장치/사용자로부터 조직의 네트워크에 대한 액세스를 제공합니다. (호)
- Cisco SD-WAN 패브릭에 포함되기 위해 각 RA 사용자의 장치가 필요하지 않은 RA 사용자에게 Cisco SD-WAN 솔루션을 확장합니다.

- 데이터 보안
- 스플릿 터널링 또는 모두 터널
- 확장성
- Cisco SD-WAN 패브릭의 여러 Cisco IOS® XE SD-WAN 장치에 RA 로드를 분산시킬 수 있습니다.

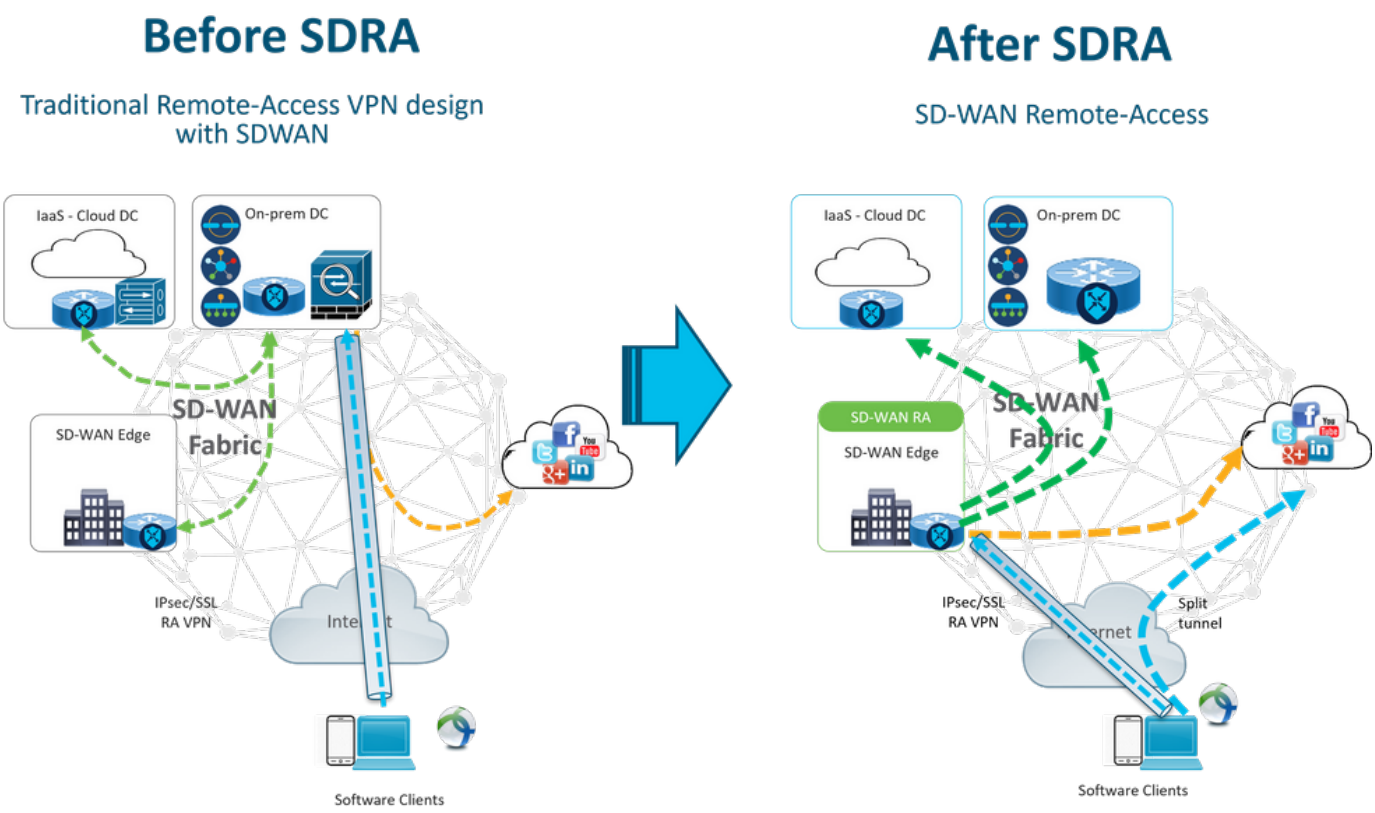
스플릿 터널링 vs 터널 모두

분할 터널링은 이미지에 표시된 대로 특정 트래픽만 터널링해야 하는 시나리오(예: SD-WAN 서브넷)에서 사용됩니다.



SDRA 이전 및 SDRA 이후

기존 원격 액세스 VPN 설계에서는 Cisco SD-WAN 패브릭 외부의 별도의 RA 인프라가 필요합니다. 이를 통해 ASA, 일반 Cisco IOS® XE 또는 서드파티 디바이스와 같은 비 SD-WAN 어플라이언스와 같은 네트워크에 대한 원격 사용자 액세스를 제공할 수 있으며, RA 트래픽은 이미지에 표시된 대로 SD-WAN 어플라이언스로 이동합니다.



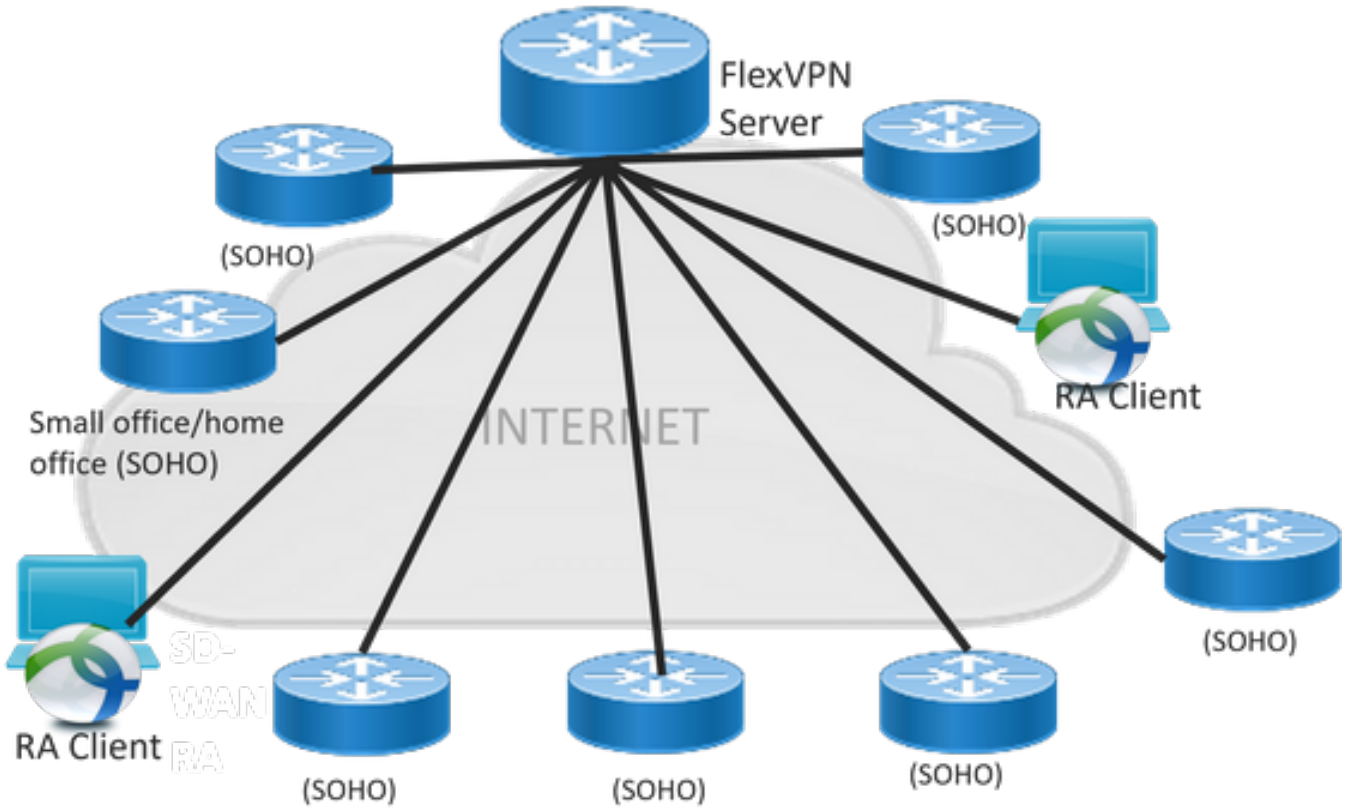
SD-WAN Remote Access는 원격 사용자가 네트워크에 연결하는 방식을 변경합니다. RA 헤드엔드로 사용되는 cEdge에 직접 연결됩니다. Cisco SD-WAN 기능 및 혜택을 RA 사용자에게 확장합니다. RA 사용자는 지사 LAN 측 사용자가 됩니다.

각 RA 클라이언트에 대해 SD-WAN RA 헤드엔드는 IP 주소를 RA 클라이언트에 할당하고 RA 사용자가 배치된 서비스 VRF의 할당된 IP 주소에 고정 호스트 경로를 추가합니다.

고정 경로는 RA 클라이언트 연결의 VPN 터널을 지정합니다. SD-WAN RA 헤드엔드는 서비스 VPN의 모든 에지 디바이스에 OMP를 사용하여 RA 클라이언트의 서비스 VRF 내의 고정 IP를 광고합니다.

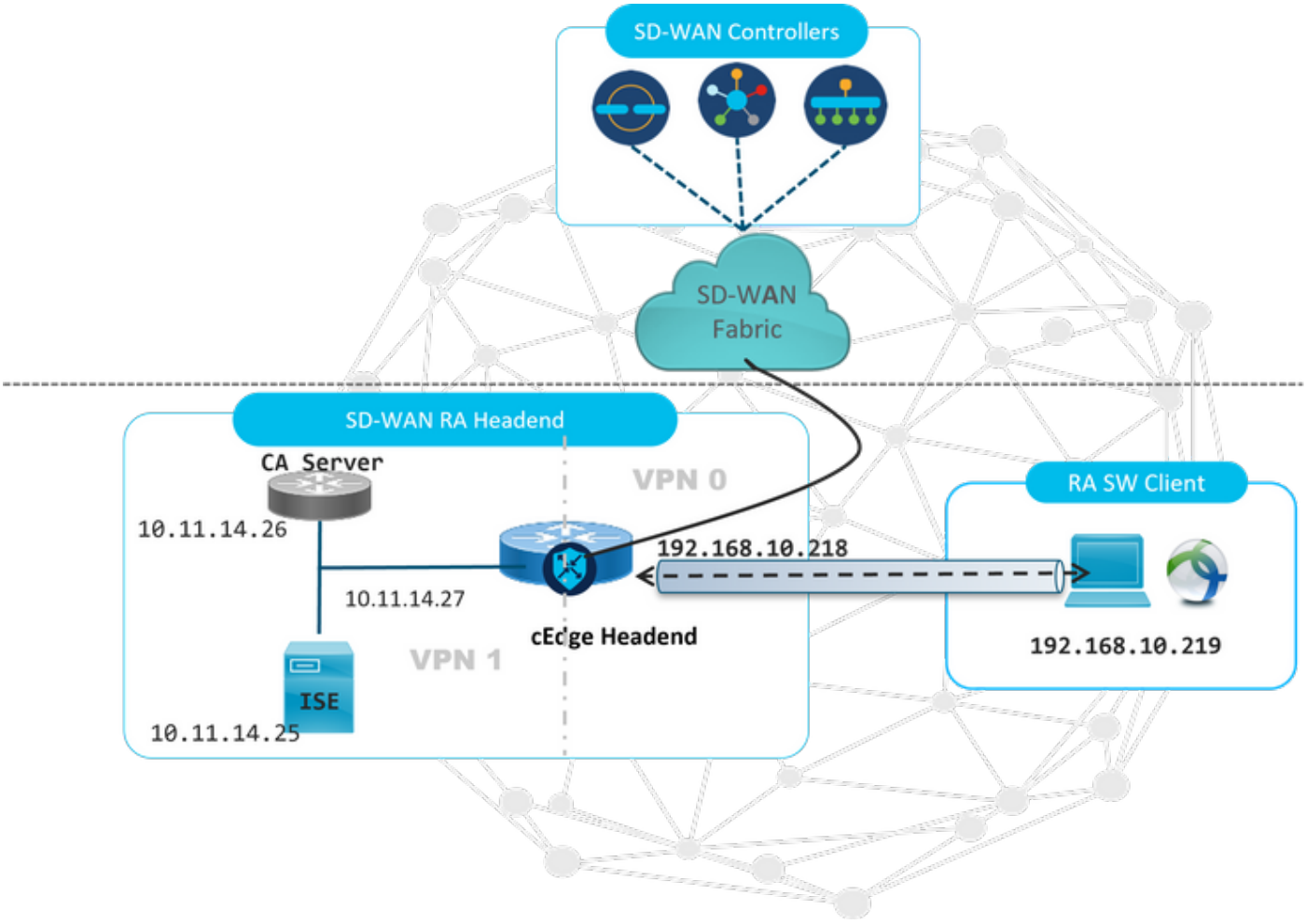
FlexVPN이란?

SD-WAN RA Cisco FlexVPN RA 솔루션을 활용합니다. FlexVPN은 Cisco가 IKEv2 표준 기능을 구현한 것으로, 사이트 간, **원격 액세스**, 허브 및 스포크 토폴로지, 부분 메시(스포크 다이렉트) 등을 결합한 통합 패러다임 및 CLI입니다. FlexVPN은 간소하지만 모듈형 프레임워크를 제공합니다. 이 프레임워크는 기존 VPN 구현과 호환되지만 터널 인터페이스 패러다임을 광범위하게 사용합니다.



필수 구성 요소

이 예에서는 이미지에 표시된 대로 SD-WAN RA 랩 설정이 생성되었습니다.



이 SD-WAN RA 랩 시나리오에 대해 추가 구성 요소가 구성되었습니다.

- CA 서버로 자동 모드의 일반 Cisco IOS® XE.
- 인증, 권한 부여 및 계정 관리를 위한 ISE/Radius 서버.
- WAN 인터페이스를 통해 cEdge에 연결할 수 있는 Windows PC.
- AnyConnect 클라이언트가 이미 설치되어 있습니다.

참고: CA 및 RADIUS 서버는 서비스 VRF 1에 배치되었습니다. 모든 SD-WAN RA 헤드엔드에 대해 서비스 VRF를 통해 두 서버에 모두 연결할 수 있어야 합니다.

참고: Cisco SD-WAN Remote Access는 17.7.1a 버전 및 SDRA용 특정 디바이스에서 지원됩니다. 지원되는 디바이스 참조의 경우 다음으로 이동합니다. SD-WAN RA 헤드엔드에 지원되는 플랫폼

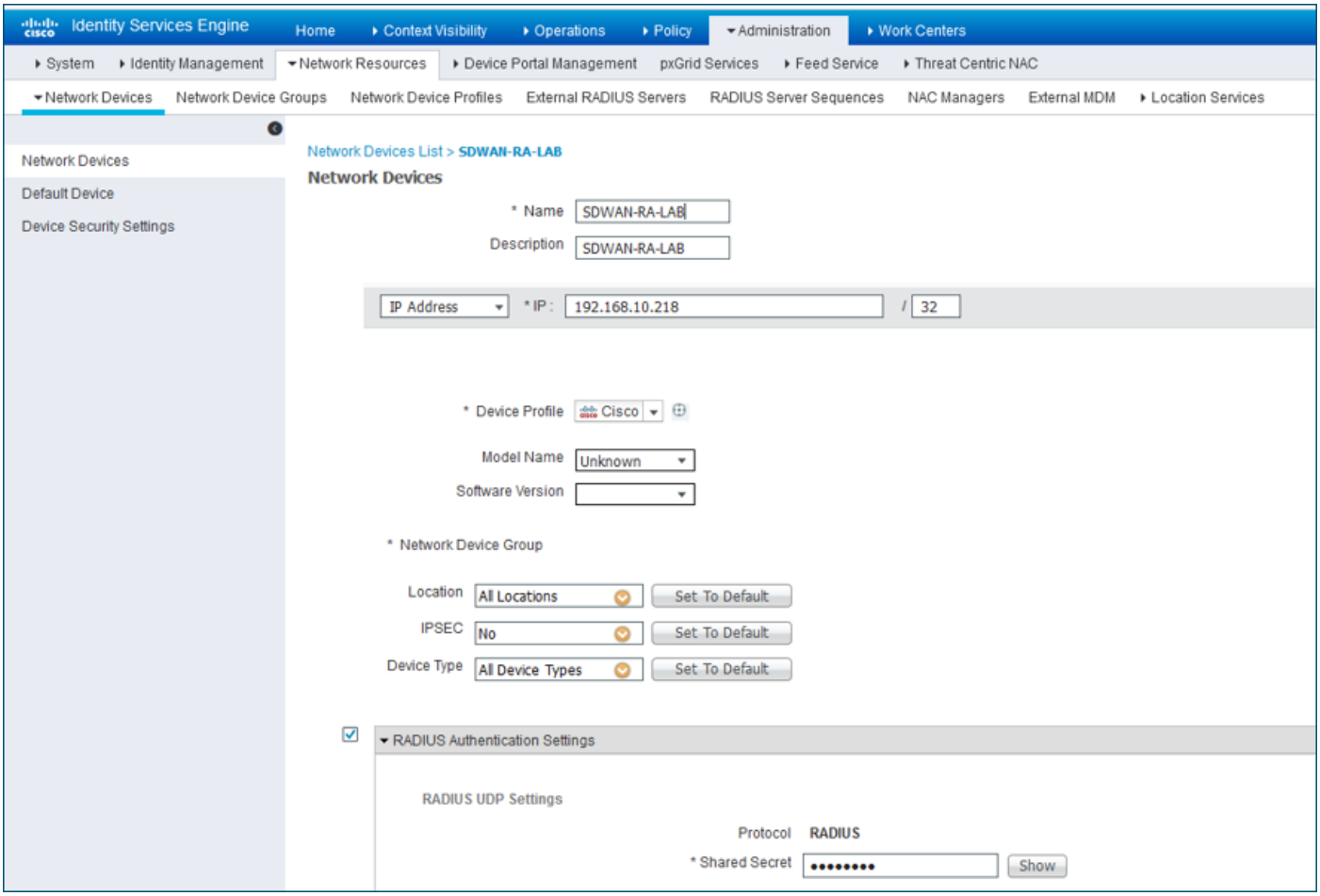
ISE 컨피그레이션

SD-WAN RA 헤드엔드를 지원하려면 매개변수가 RADIUS 서버에 구성되어 있는지 확인합니다. 다음 매개변수는 RA 연결에 필요합니다.

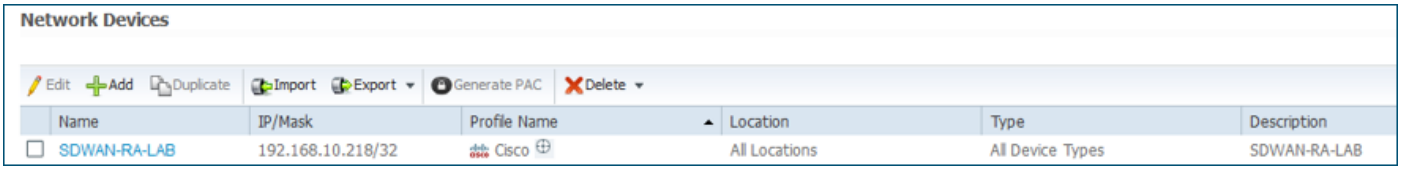
- 사용자 인증 자격 증명 AnyConnect-EAP 연결을 위한 사용자 이름 및 비밀번호
- 사용자 또는 사용자 그룹에 적용되는 정책 매개변수(특성) **VRF**: RA 사용자가 할당된 서비스 VPN**IP 풀 이름**: RA 헤드엔드에 정의된 IP 풀의 이름**서버 서브넷**: RA 사용자에게 제공할 서브넷 액세스

ISE에서 구성하는 첫 번째 단계는 RADIUS를 ISE에 요청할 수 있는 네트워크 디바이스로서 RA 헤드엔드 또는 cEdge IP 주소입니다.

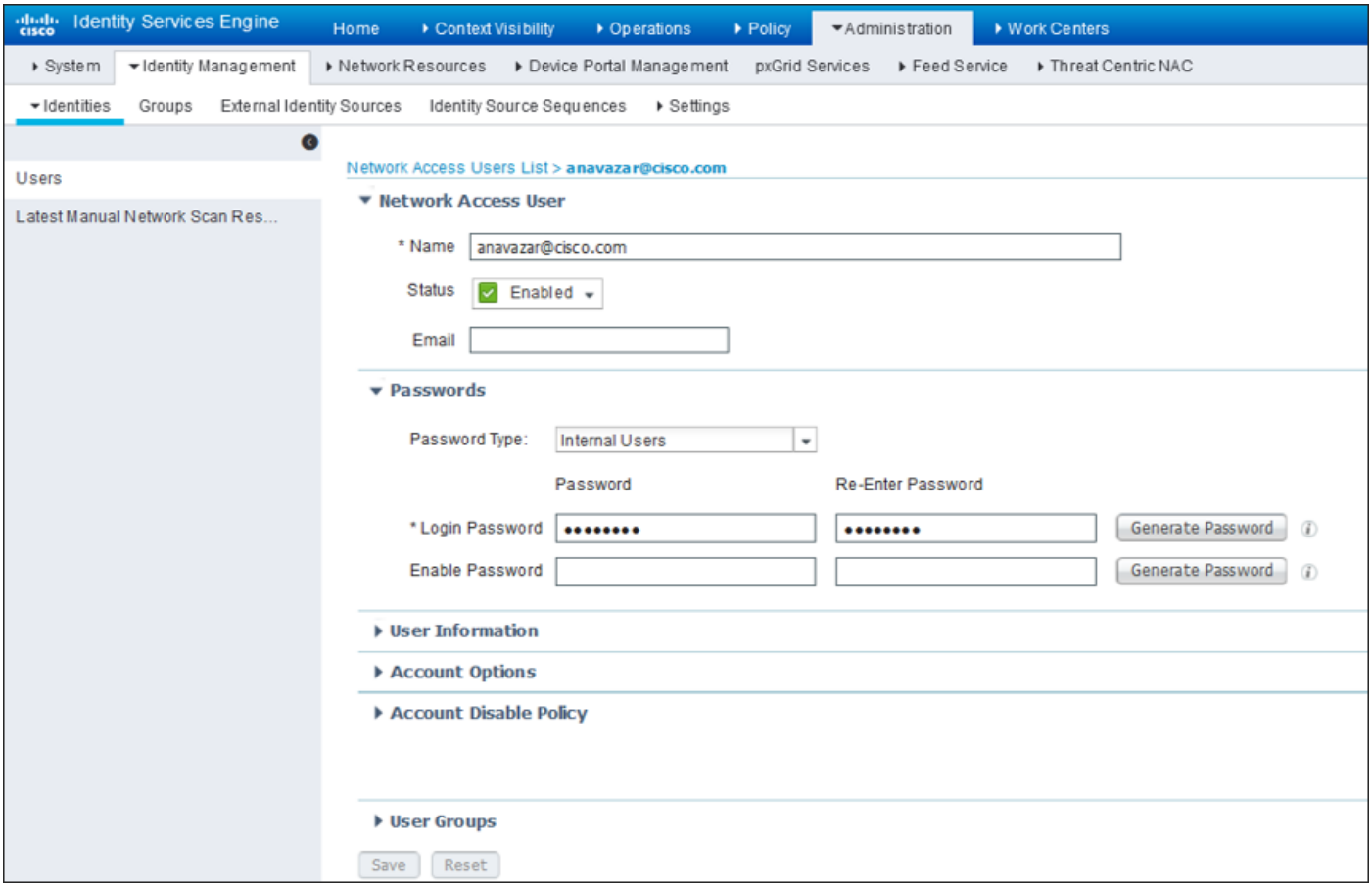
Administration(**관리) > Network Devices(네트워크 디바이스**)로 이동하고 이미지에 표시된 대로 RA Headed(cEdge) IP 주소와 비밀번호를 추가합니다.



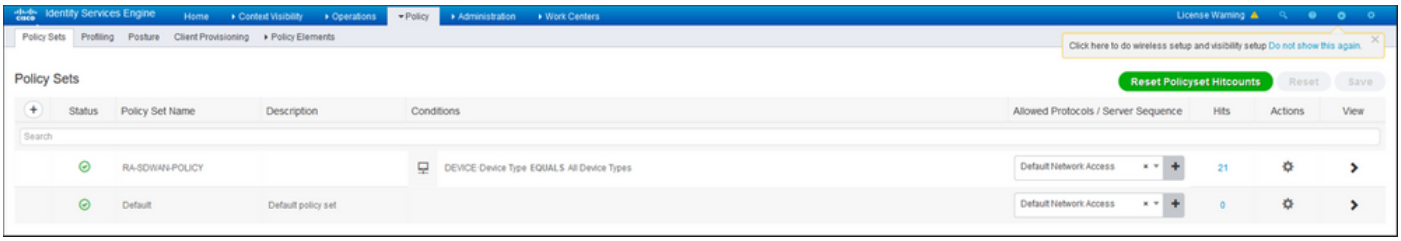
이미지에 표시된 대로 네트워크 디바이스가 추가되었습니다.



이미지에 표시된 대로 AnyConnect 인증을 위한 사용자 이름 및 비밀번호를 구성하려면 RADIUS 서버가 필요합니다. Administration(관리) > **Identities(ID)**로 **이동합니다**.



이미지에 표시된 대로 적중하려면 일치 조건으로 정책 세트를 생성해야 합니다. 이 경우 **모든 디바이스 유형** 조건이 사용되므로 모든 사용자가 이 정책을 적용했습니다.



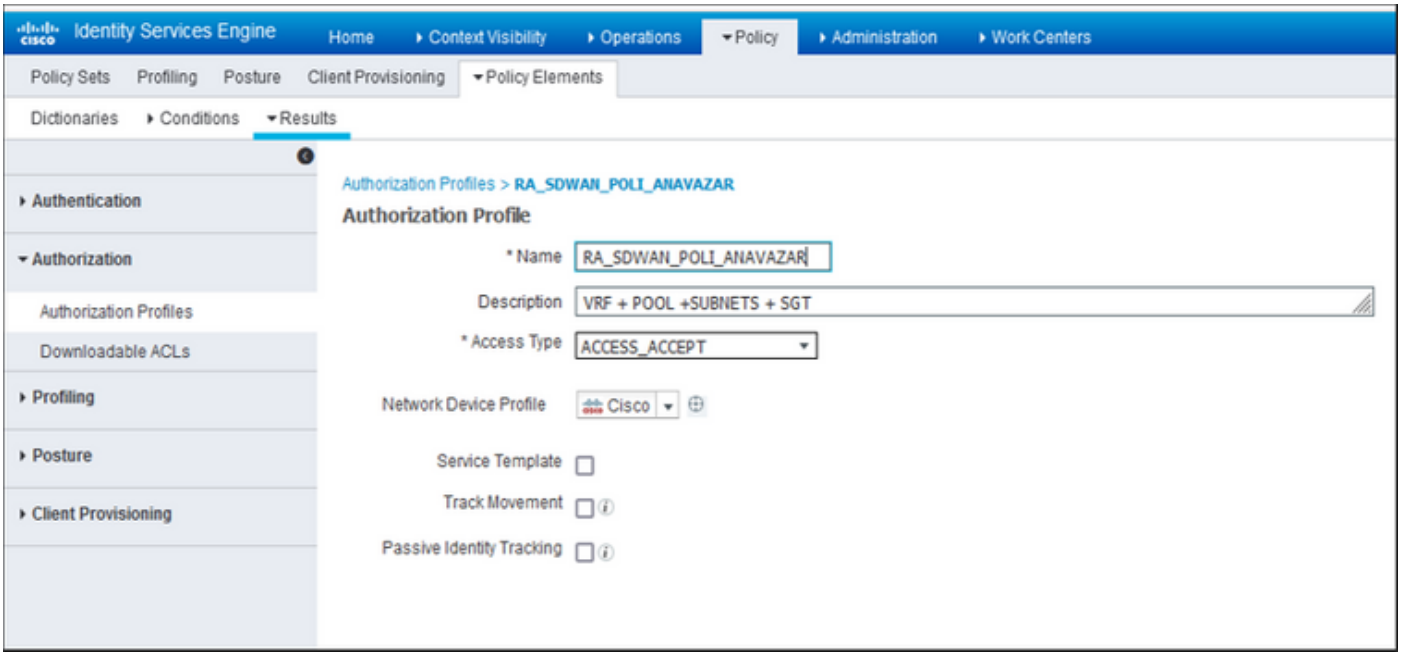
그런 다음 Authorization Policy(권한 부여 정책)가 조건당 하나씩 생성되었습니다. All Device **types(모든 디바이스 유형)** 및 일치시킬 Identity group(ID 그룹) 조건

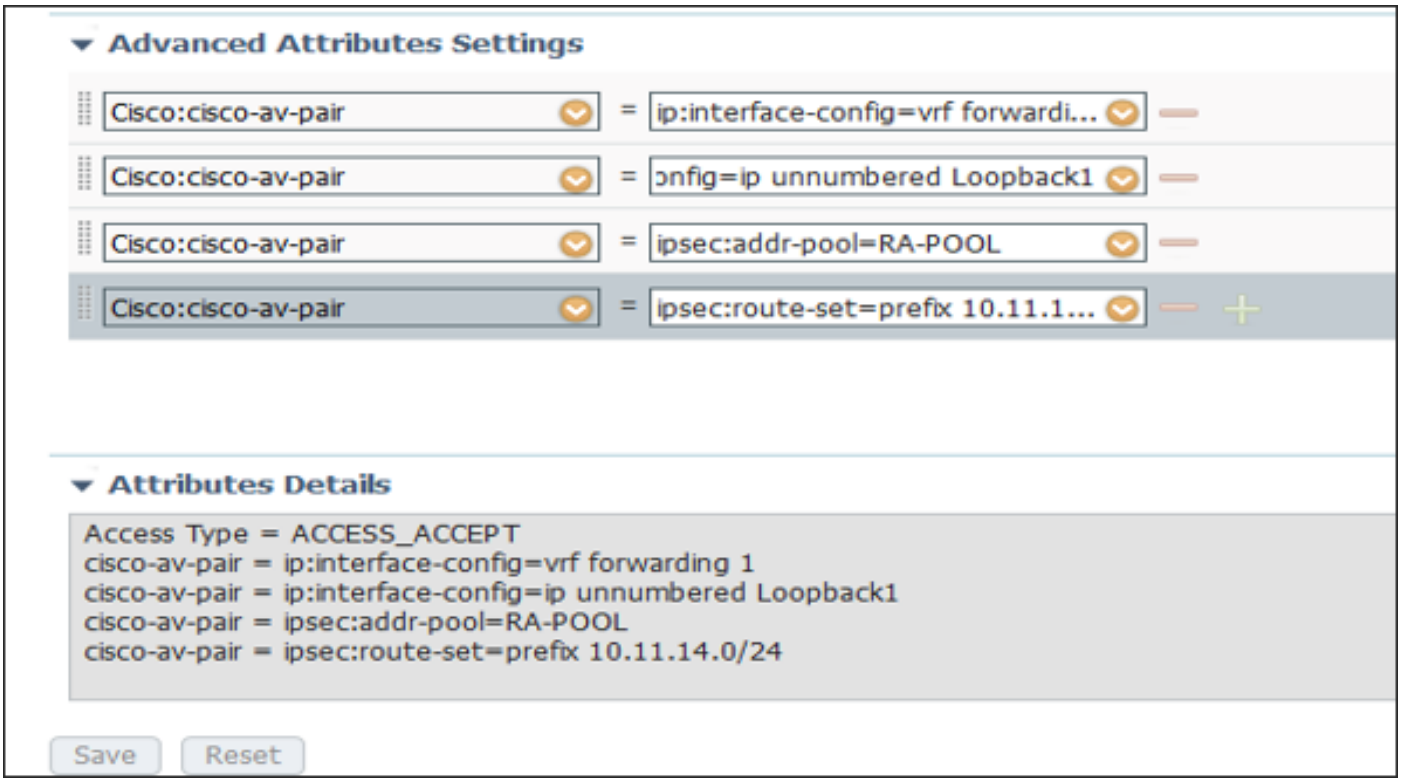
Authorization **Profile(권한 부여 프로파일)**에서 Advanced Attributes Settings(고급 특성 설정) **아래에서 Access_ACCEPT로 Access**(액세스 유형)를 Cisco 벤더 및 **Cisco-AV-pair 특성을 선택해야 합니다.**

사용자에 대한 일부 정책 매개변수를 구성해야 합니다.

- 사용자가 속한 서비스 VRF인 VRF입니다.
- IP 풀 이름, 각 사용자 연결에는 cEdge에 구성된 IP 풀에 속하는 IP 주소가 할당됩니다.
- 사용자가 액세스할 수 있는 서브넷

주의: IP vrf **forwarding** 명령은 **IP unnumbered** 명령 앞에 와야 합니다. 가상 액세스 인터페이스가 가상 템플릿에서 복제되고 **IP vrf forwarding** 명령이 적용되면 가상 액세스 인터페이스에서 모든 IP 컨피그레이션이 제거됩니다.





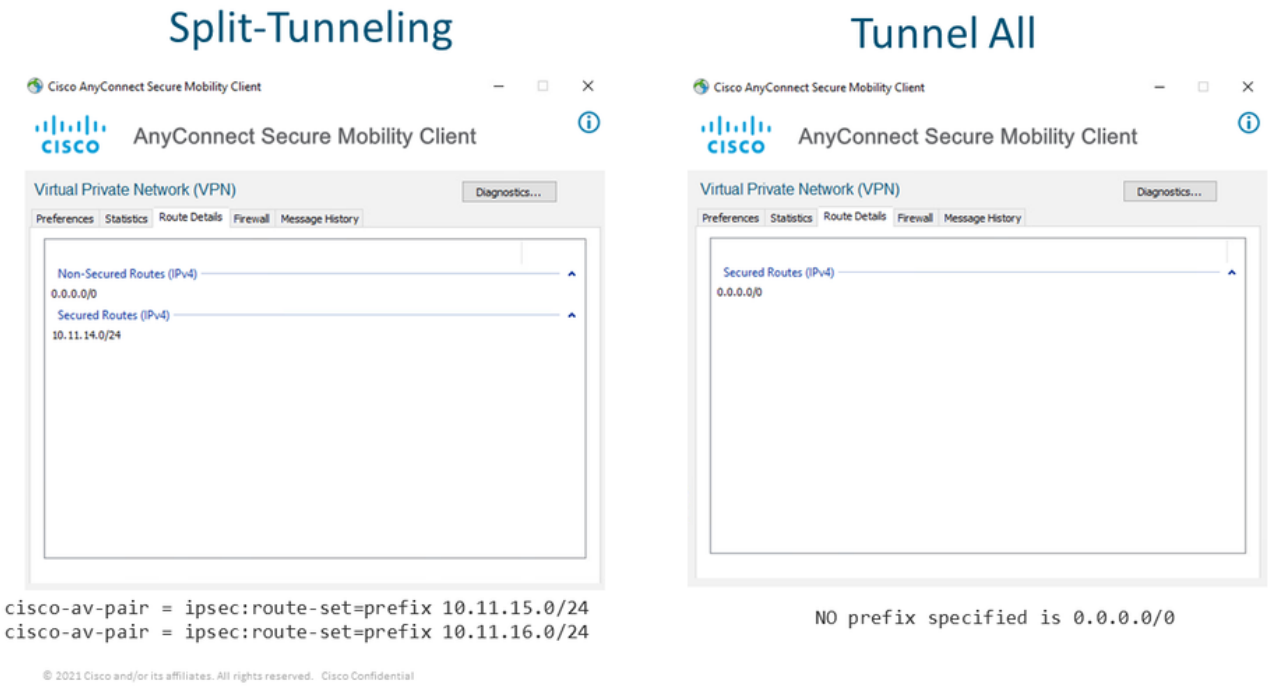
사용자 특성:

```
Access Type = ACCESS_ACCEPT
cisco-av-pair = ip:interface-config=vrf forwarding 1
cisco-av-pair = ip:interface-config=ip unnumbered Loopback1
```

```
cisco-av-pair = ipsec:addr-pool=RA-POOL
cisco-av-pair = ipsec:route-set=prefix 10.11.15.0/24
cisco-av-pair = ipsec:route-set=prefix 10.11.16.0/24
```

AnyConnect 클라이언트에서 스플릿 터널링 대 모두 터널

ipsec:route-set=AnyConnect 클라이언트에서 받은 접두사 특성이 이미지에 표시된 대로 설치됩니다.



Cisco IOS® XE의 CA 서버 컨피그레이션

CA 서버는 Cisco IOS® XE SD-WAN 디바이스에 인증서를 프로비저닝하고 RA 헤드엔드에서 RA 클라이언트에 자신을 인증할 수 있도록 합니다.

이러한 crypto PKI 서버 명령은 Cisco IOS® XE SD-WAN에서 지원되지 않으므로 CEEDGE는 CA 서버가 될 수 없습니다.

- RSA 키 쌍 생성
- CA 서버에 대한 PKI 신뢰 지점 생성 이전에 생성한 KEY-CA를 사용하여 rsakeypair를 구성합니다.

  참고: PKI 서버와 PKI 신뢰 지점은 동일한 이름을 사용해야 합니다.

- CA 서버 생성 CA 서버의 발급자 이름 구성"No shutdown"을 사용하여 CA 서버를 활성화합니다.

```
crypto key generate rsa modulus 2048 label KEY-CA
!
```

```
crypto pki trustpoint CA
 revocation-check none
 rsakeypair KEY-CA
 auto-enroll
!
crypto pki server CA
 no database archive
 issuer-name CN=CSR1Kv_SDWAN_RA
 grant auto
 hash sha1
 lifetime certificate 3600
 lifetime ca-certificate 3650
 auto-rollover
no shutdown
!
```

CA 서버가 활성화되었는지 확인합니다.

```
CA-Server-CSRv#show crypto pki server CA
Certificate Server CA:
    Status: enabled
    State: enabled
   Server's configuration is locked  (enter "shut" to unlock it)
   Issuer name: CN=CSR1Kv_SDWAN_RA
   CA cert fingerprint: 10DA27AD EF54A3F8 12925750 CE2E27EB
   Granting mode is: auto
   Last certificate issued serial number (hex): 3
   CA certificate expiration timer: 23:15:33 UTC Jan 17 2032
   CRL NextUpdate timer: 05:12:12 UTC Jan 22 2022
   Current primary storage dir: nvram:
   Database Level: Minimum - no cert data written to storage
   Auto-Rollover configured, overlap period 30 days
   Autorollover timer: 23:15:37 UTC Dec 18 2031
```

CA 서버 인증서가 설치되어 있는지 확인합니다.

```
CA-Server-CSRv#show crypto pki certificates verbose CA
CA Certificate
 Status: Available
 Version: 3
 Certificate Serial Number (hex): 01
 Certificate Usage: Signature
 Issuer:
 cn=CSR1Kv_SDWAN_RA
 Subject:
 cn=CSR1Kv_SDWAN_RA
 Validity Date:
 start date: 23:15:33 UTC Jan 19 2022
 end date: 23:15:33 UTC Jan 17 2032
 Subject Key Info:
 Public Key Algorithm: rsaEncryption
 RSA Public Key: (2048 bit)
 Signature Algorithm: SHA1 with RSA Encryption
 Fingerprint MD5: 10DA27AD EF54A3F8 12925750 CE2E27EB
 Fingerprint SHA1: 44E256C3 4FA45C5D F0398630 9D88B75E 5026CE4A
 X509v3 extensions:
 X509v3 Key Usage: 86000000
 Digital Signature
 Key Cert Sign
 CRL Signature
 X509v3 Subject Key ID: 92F7CD72 355AA85F 672867D4 EC0C10C5 0B177C38
 X509v3 Basic Constraints:
```

```
 CA: TRUE
 X509v3 Authority Key ID: 92F7CD72 355AA85F 672867D4 EC0C10C5 0B177C38
 Authority Info Access:
Cert install time: 23:44:35 UTC Mar 13 2022
Associated Trustpoints: -RA-truspoint CA
Storage: nvram:CSR1Kv_SDWAN#1CA.cer
```

CA 인증서**의 핑거프린트 SHA 1**은 원격 액세스 컨피그레이션과 함께 cEdge 라우터(RA 헤드엔드)의 **crypto pki 신뢰 지점**에서 사용됩니다.

```
Fingerprint SHA1: 44E256C3 4FA45C5D F0398630 9D88B75E 5026CE4A
```

SD-WAN RA 컨피그레이션

> **참고:** 이 문서에서는 컨트롤러 및 cEdge의 SD-WAN 온보딩 프로세스에 대해 다루지 않습니다. SD-WAN 패브릭이 작동 중이고 완벽하게 작동하는 것으로 간주됩니다.

Crypto PKI 컨피그레이션

- PKI 신뢰 지점을 만듭니다.
- CA 서버의 URL을 구성합니다.
- CA 서버 인증서에서 지문 sha 1을 복사합니다.
- 새 ID 인증서에 대한 주체 이름 및 대체 이름을 구성합니다.
- 이전에 생성된 KEY-ID로 rsakeypar을 구성합니다.

```
crypto pki trustpoint RA-TRUSTPOINT
 subject-name CN=cEdge-SDWAN-1.crv
 enrollment url http://10.11.14.226:80
 fingerprint 44E256C34FA45C5DF03986309D88B75E5026CE4A
 subject-name CN=cEdge-SDWAN-1.crv
 vrf 1
 rsakeypair KEY-NEW
 revocation-check none
```

인증할 CA 인증서 요청:

```
crypto pki authenticate RA-TRUSTPOINT
```

CSR을 생성하고 CA 서버로 전송하며 새 ID 인증서를 받습니다.

```
Crypto pki enroll RA-TRUSTPOINT
```

CA 인증서 및 cEdge 인증서를 확인합니다.

```
cEdge-207#show crypto pki certificates RA-TRUSTPOINT
Certificate
 Status: Available
 Certificate Serial Number (hex): 04
 Certificate Usage: General Purpose
 Issuer:
   cn=CSR1Kv_SDWAN_RA
```

```
 Subject:
   Name: cEdge-207
   hostname=cEdge-207
   cn=cEdge-SDWAN-1.crv
 Validity Date:
   start date: 03:25:40 UTC Jan 24 2022
   end   date: 03:25:40 UTC Dec 3 2031
 Associated Trustpoints: RA-TRUSTPOINT
 Storage: nvram:CSR1Kv_SDWAN#4.cer
CA Certificate
 Status: Available
 Certificate Serial Number (hex): 01
 Certificate Usage: Signature
 Issuer:
   cn=CSR1Kv_SDWAN_RA
 Subject:
   cn=CSR1Kv_SDWAN_RA
 Validity Date:
   start date: 23:15:33 UTC Jan 19 2022
   end   date: 23:15:33 UTC Jan 17 2032
 Associated Trustpoints: RA-TRUSTPOINT
Storage: nvram:CSR1Kv_SDWAN#1CA.cer
```

AAA 컨피그레이션

```
aaa new-model
!
aaa group server radius ISE-RA-Group
 server-private 10.11.14.225 key Cisc0123
 ip radius source-interface GigabitEthernet2
!
aaa authentication login ISE-RA-Authentication group ISE-RA-Group
aaa authorization network ISE-RA-Authorization group ISE-RA-Group
aaa accounting network ISE-RA-Accounting start-stop group ISE-RA-Group
```

FlexVPN 컨피그레이션

IP 풀 구성

```
ip local pool RA-POOL 10.20.14.1 10.20.14.100
```

IKEv2 제안서(암호 및 매개변수) 및 정책을 구성합니다.

```
crypto ikev2 proposal IKEV2-RA-PROP
 encryption aes-cbc-256
 integrity sha256
 group 19
 prf sha256

crypto ikev2 policy IKEV2-RA-POLICY
 proposal IKEV2-RA-PROP
```

IKEv2 프로파일 이름 관리자를 구성합니다.

```
crypto ikev2 name-mangler IKEV2-RA-MANGLER
 eap suffix delimiter @
```

참고: name-mangler는 접두사와 접미어를 분리하는 EAP ID의 EAP ID(사용자 이름) 구분 기

호 접두사에서 이름을 파생합니다.

IPsec 암호를 구성합니다.

```
crypto ipsec transform-set IKEV2-RA-TRANSFORM-SET esp-aes 256 esp-sha-hmac
 mode tunnel
```

암호화 IKEv2 프로필 구성:

```
crypto ikev2 profile RA-SDWAN-IKEV2-PROFILE
 match identity remote any
 identity local address 192.168.10.218
 authentication local rsa-sig
 authentication remote anyconnect-eap aggregate
 pki trustpoint RA-TRUSTPOINT
 aaa authentication anyconnect-eap ISE-RA-Authentication
 aaa authorization group anyconnect-eap list ISE-RA-Authorization name-mangler IKEV2-RA-MANGLER
password Cisc0123456
 aaa authorization user anyconnect-eap list ISE-RA-Authorization USER-SDWAN password Us3r123456
 aaa accounting anyconnect-eap ISE-RA-Accounting
```

Crypto IPSEC 프로필 구성:

```
crypto ipsec profile IKEV2-RA-PROFILE
 set transform-set IKEV2-RA-TRANSFORM-SET
 set ikev2-profile RA-SDWAN-IKEV2-PROFILE
```

가상 템플릿 인터페이스 구성:

```
!
interface Virtual-Template101 type tunnel
 vrf forwarding 1
 tunnel mode ipsec ipv4
 tunnel protection ipsec profile IKEV2-RA-PROFILE
```

Crypto IKEv2 프로필에서 가상 템플릿을 구성합니다.

```
crypto ikev2 profile RA-SDWAN-IKEV2-PROFILE
 virtual-template 101
```

SD-WAN RA 컨피그레이션 예

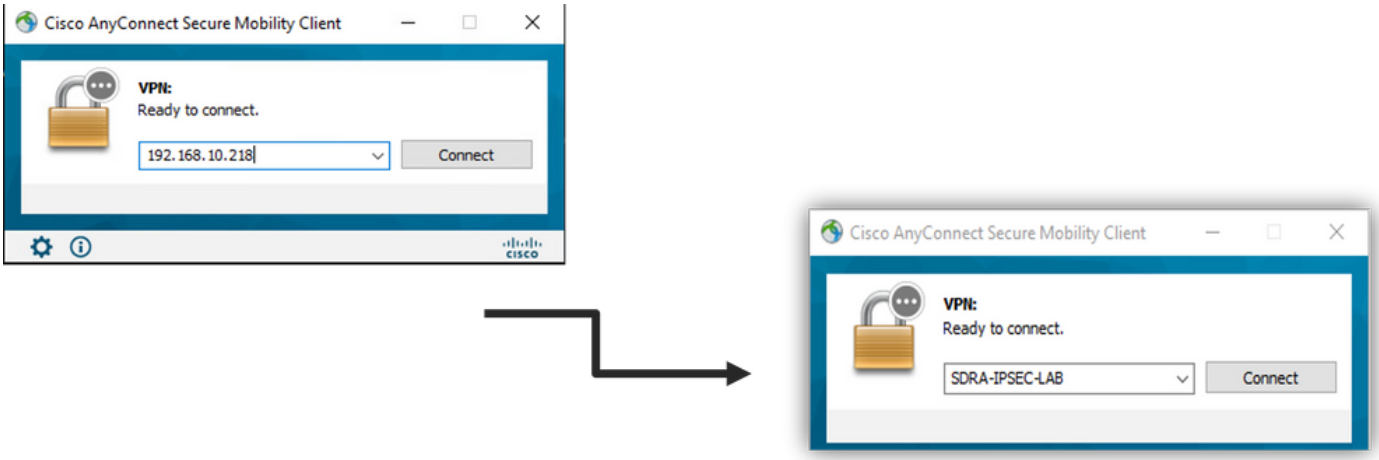
```
aaa new-model
!
aaa group server radius ISE-RA-Group
server-private 10.11.14.225 key Cisc0123
!
aaa authentication login ISE-RA-Authentication group ISE-RA-Group
aaa authorization network ISE-RA-Authorization group ISE-RA-Group
aaa accounting network ISE-RA-Accounting start-stop group ISE-RA-Group
!
crypto pki trustpoint RA-TRUSTPOINT
 subject-name CN=cEdge-SDWAN-1.crv
```

```
 enrollment url http://10.11.14.226:80
 fingerprint 44E256C34FA45C5DF03986309D88B75E5026CE4A
 subject-name CN=cEdge-SDWAN-1.crv
 vrf 1
 rsakeypair KEY-NEW
 revocation-check none
!
ip local pool RA-POOL 10.20.14.1 10.20.14.100
!
crypto ikev2 name-mangler IKEV2-RA-MANGLER
 eap suffix delimiter @
!
crypto ikev2 proposal IKEV2-RA-PROP
 encryption aes-cbc-256
 integrity sha256
 group 19
 prf sha256
!
crypto ikev2 policy IKEV2-RA-POLICY
 proposal IKEV2-RA-PROP
!
crypto ipsec transform-set IKEV2-RA-TRANSFORM-SET esp-aes 256 esp-sha-hmac
 mode tunnel
!
crypto ikev2 profile RA-SDWAN-IKEV2-PROFILE
 match identity remote any
 identity local address 192.168.10.218
 authentication local rsa-sig
 authentication remote anyconnect-eap aggregate
 pki trustpoint RA-TRUSTPOINT
 aaa authentication anyconnect-eap ISE-RA-Authentication
 aaa authorization group anyconnect-eap list ISE-RA-Authorization name-mangler IKEV2-RA-MANGLER
password Cisc0123456
 aaa authorization user anyconnect-eap list ISE-RA-Authorization USER-SDWAN password Us3r123456
 aaa accounting anyconnect-eap ISE-RA-Accounting
!
crypto ipsec profile IKEV2-RA-PROFILE
 set transform-set IKEV2-RA-TRANSFORM-SET
 set ikev2-profile RA-SDWAN-IKEV2-PROFILE
!
interface Virtual-Template101 type tunnel
 vrf forwarding 1
 tunnel mode ipsec ipv4
 tunnel protection ipsec profile IKEV2-RA-PROFILE
!
crypto ikev2 profile RA-SDWAN-IKEV2-PROFILE
 virtual-template 101
```

AnyConnect 클라이언트 컨피그레이션

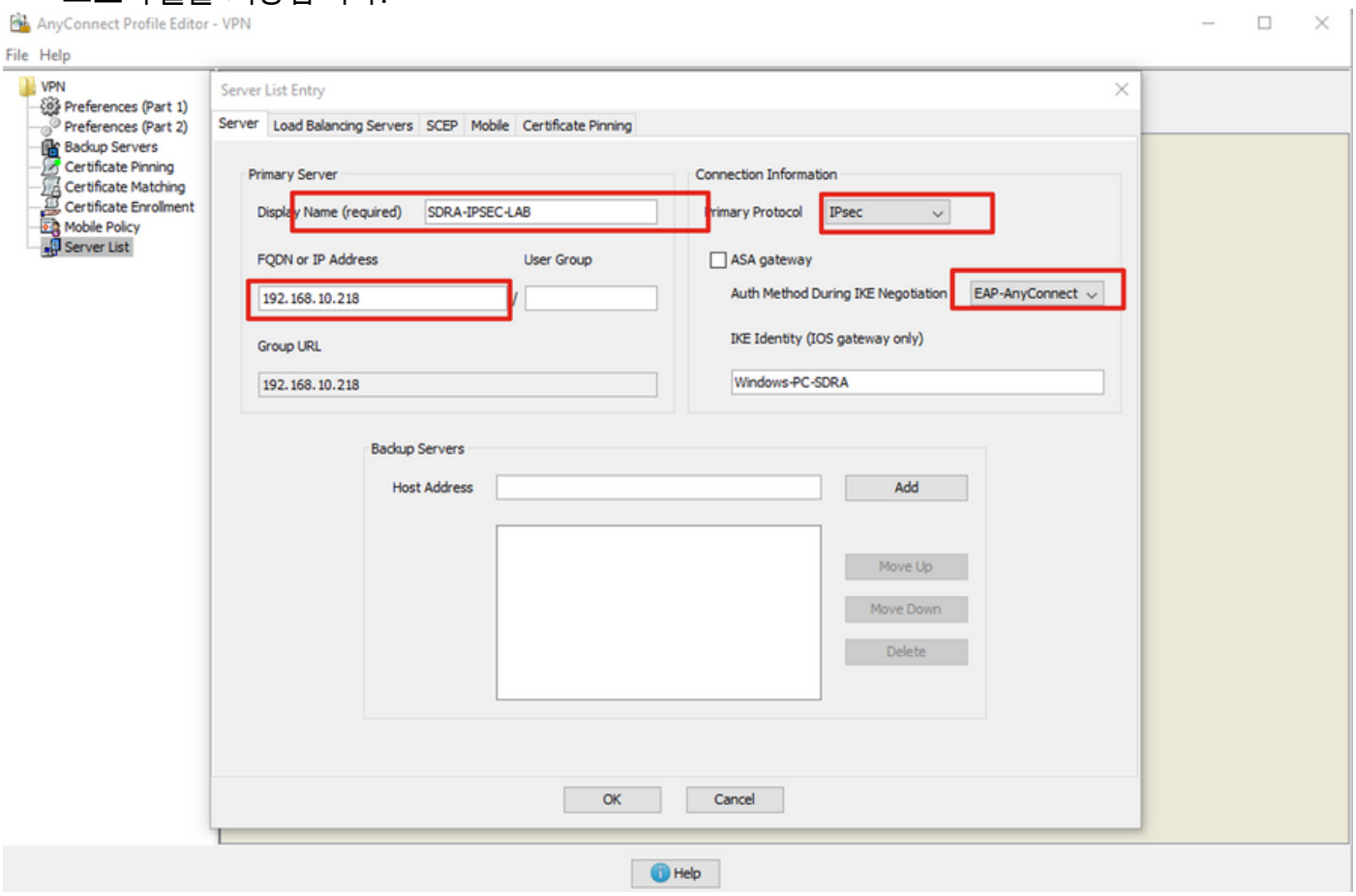
AnyConnect 클라이언트는 SSL을 터널 설정의 기본 프로토콜로 사용하며 이 프로토콜은 SD-WAN RA(로드맵)에 대해 지원되지 않습니다. RA는 FlexVPN을 사용하므로 IPSEC은 사용되는 프로토콜이며 반드시 변경해야 하며 XML 프로파일을 통해 수행됩니다.

사용자는 AnyConnect 클라이언트의 주소 표시줄에 VPN 게이트웨이의 FQDN을 수동으로 입력할 수 있습니다. 그러면 게이트웨이에 대한 SSL 연결이 생성됩니다.



AnyConnect 프로파일 편집기 구성

- Server **List(서버 목록)로** 이동하고 Add(추가)를 **클릭합니다**.
- IPsec**을** "Primary Protocol"로 선택합니다.
- **ASA 게이트웨이** 옵션의 선택을 취소합니다.
- EAP-**AnyConnect를** "IKE 협상 중 인증 방법"으로 선택합니다.
- **Display/Name(필수)**은 AnyConnect 클라이언트 아래에 이 연결을 저장하는 데 사용되는 이름입니다.
- **FQDN 또는 IP 주소는** cEdge(공용) IP 주소로 작성해야 합니다.
- 프로파일을 저장합니다.



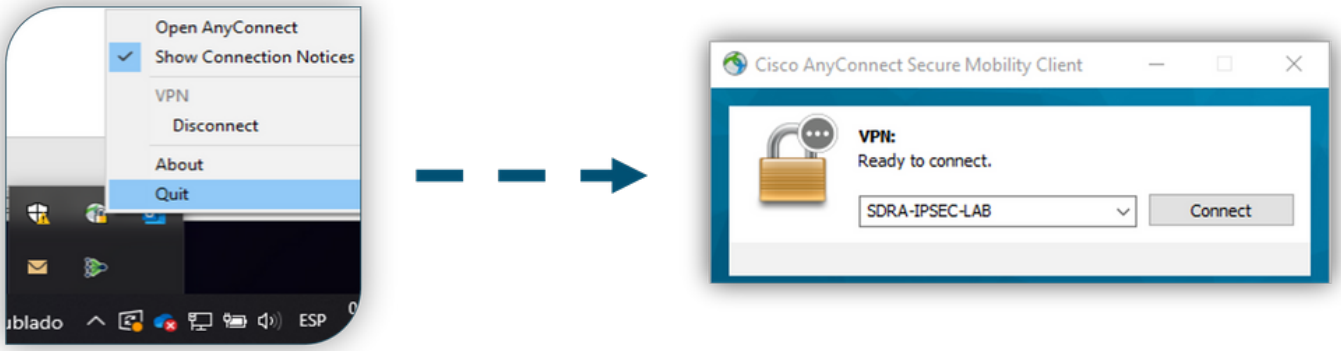
AnyConnect 프로파일(XML) 설치

XML 프로파일을 디렉토리에 수동으로 넣을 수 있습니다.

```
For Windows:
C:\ProgramData\Cisco\Cisco AnyConnect Secure Mobility Client\Profile

For MAC OS:
/opt/cisco/anyconnect/profile
```

프로파일을 GUI에 표시하려면 AnyConnect 클라이언트를 다시 시작해야 합니다. Windows 트레이에서 AnyConnect 아이콘을 마우스 오른쪽 버튼으로 클릭하고 Quit(종료) 옵션을 선택하여 프로세스를 다시 시작할 수 **있습니다.**



AnyConnect 다운로더 비활성화

AnyConnect 클라이언트는 기본적으로 성공적으로 로그인한 후 XML 프로파일 다운로드를 시도합니다.

프로파일을 사용할 수 없으면 연결이 실패합니다. 이를 해결하려면 클라이언트 자체에서 AnyConnect 프로파일 다운로드 기능을 비활성화할 수 있습니다.

Windows의 경우:

```
C:\ProgramData\Cisco\Cisco AnyConnect Secure Mobility Client\AnyConnectLocalPolicy.xml
```

MAC OS의 경우:

```
/opt/cisco/anyconnect/AnyConnectLocalPolicy.xml
```

"BypassDownloader" 옵션은 "true"로 설정됩니다.

```
<?xml version="1.0" encoding="UTF-8"?>
<AnyConnectLocalPolicy xmlns="http://schemas.xmlsoap.org/encoding/"
xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"
xsi:schemaLocation="http://schemas.xmlsoap.org/encoding/ AnyConnectLocalPolicy.xsd"
acversion="4.9.04043">
<BypassDownloader>true</BypassDownloader>
<EnableCRLCheck>false</EnableCRLCheck>
<ExcludeFirefoxNSSCertStore>false</ExcludeFirefoxNSSCertStore>
<ExcludeMacNativeCertStore>false</ExcludeMacNativeCertStore>
<ExcludePemFileCertStore>false</ExcludePemFileCertStore>
<ExcludeWinNativeCertStore>false</ExcludeWinNativeCertStore>
<FipsMode>false</FipsMode>
<RestrictPreferenceCaching>false</RestrictPreferenceCaching>
<RestrictServerCertStore>false</RestrictServerCertStore>
```

```
<RestrictTunnelProtocols>false</RestrictTunnelProtocols>
<RestrictWebLaunch>false</RestrictWebLaunch>
<StrictCertificateTrust>false</StrictCertificateTrust>
<UpdatePolicy>
<AllowComplianceModuleUpdatesFromAnyServer>true</AllowComplianceModuleUpdatesFromAnyServer>
<AllowISEProfileUpdatesFromAnyServer>true</AllowISEProfileUpdatesFromAnyServer>
<AllowManagementVPNProfileUpdatesFromAnyServer>true</AllowManagementVPNProfileUpdatesFromAnyServ
er>
<AllowServiceProfileUpdatesFromAnyServer>true</AllowServiceProfileUpdatesFromAnyServer>
<AllowSoftwareUpdatesFromAnyServer>true</AllowSoftwareUpdatesFromAnyServer>
<AllowVPNProfileUpdatesFromAnyServer>true</AllowVPNProfileUpdatesFromAnyServer></UpdatePolicy>
</AnyConnectLocalPolicy>
```

AnyConnect 클라이언트에서 신뢰할 수 없는 서버 차단 해제

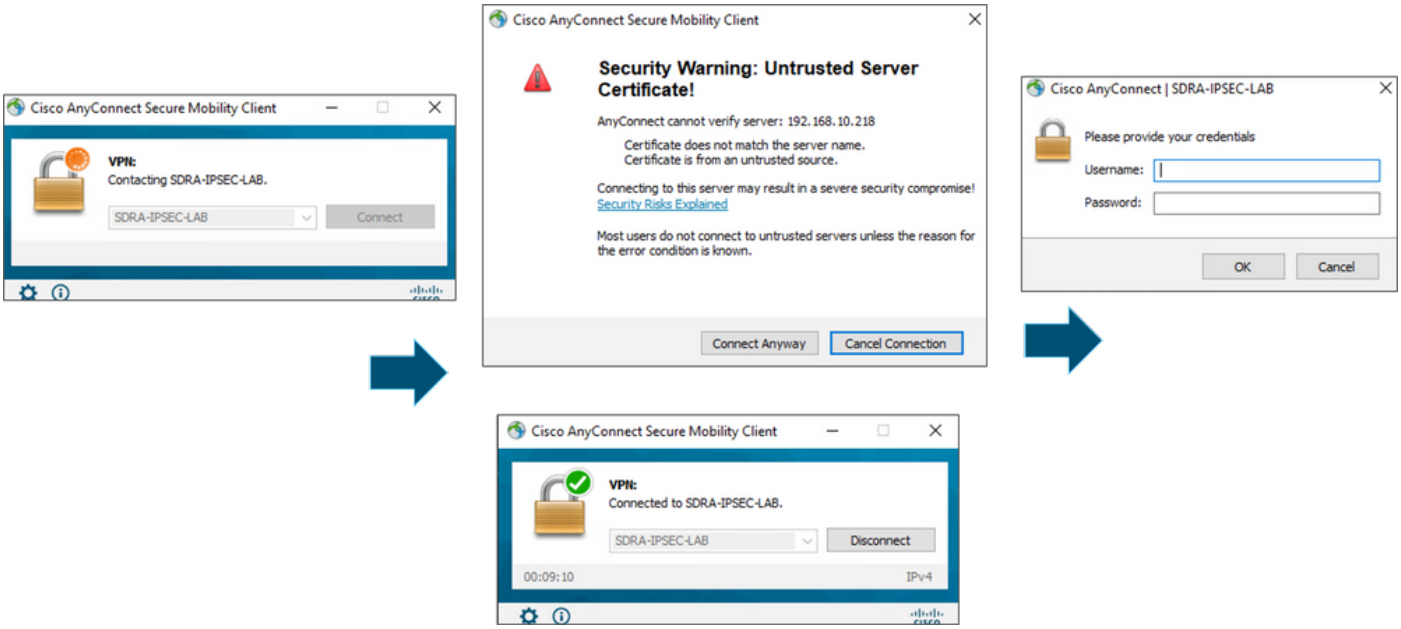
Settings(**설정**) > **Preferences(기본 설정)**로 이동하고 모든 상자 옵션의 선택을 취소합니다.

가장 중요한 것은 이 시나리오의 "**신뢰할 수 없는 서버에 대한 연결 차단**"입니다.

> **참고:** RA 헤드엔드/cEdge 인증에 사용되는 인증서는 Cisco IOS® XE의 CA 서버에서 이전에 생성하고 서명한 인증서입니다. 이 CA 서버는 GoDaddy, Symantec, Cisco 등과 같은 공용 엔터티가 아닙니다. PC 클라이언트는 인증서를 신뢰할 수 없는 서버로 해석합니다. 이는 회사에서 신뢰하는 공용 인증서 또는 CA 서버를 사용하여 수정되었습니다.

AnyConnect 클라이언트 사용

모든 SDRA 컨피그레이션이 배치되면 성공적인 연결을 위한 플로우가 이미지로 표시됩니다.



다음을 확인합니다.

가상 템플릿 인터페이스는 가상 액세스 인터페이스를 생성하여 암호화 채널을 시작하고 서버(cEdge)와 클라이언트(AnyConnect 사용자) 간에 IKEv2 및 IPsec 보안 연결(SA)을 설정하는 데 사용됩니다.

> **참고:** 가상 템플릿 인터페이스는 항상 **작동/중단됩니다**. **상태**가 **작동** 중이고 **프로토콜**이 **다운되었습니다**.

```
cEdge-207#show ip int brief
Interface              IP-Address      OK? Method Status                Protocol
GigabitEthernet1       unassigned      YES unset  up                    up
GigabitEthernet2       192.168.10.218  YES other  up                    up
GigabitEthernet3       10.11.14.227    YES other  up                    up
Sdwan-system-intf      10.1.1.18        YES unset  up                     up
Loopback1              192.168.50.1    YES other  up                    up
Loopback65528          192.168.1.1     YES other  up                    up
NVI0                   unassigned      YES unset  up                    up
Tunnel2                192.168.10.218  YES TFTP   up                    up
Virtual-Access1        192.168.50.1    YES unset  up                    up
Virtual-Template101    unassigned      YES unset  up                    down
```

show derived-config interface virtual-access <number>가 있는 클라이언트와 연결된 Virtual-Access 인터페이스에 적용된 실제 **컨피그레이션을 확인합니다**.

```
cEdge-207#show derived-config interface virtual-access 1
Building configuration...
Derived configuration : 252 bytes
!
interface Virtual-Access1
 vrf forwarding 1
 ip unnumbered Loopback1
 tunnel source 192.168.10.218
 tunnel mode ipsec ipv4
```

```
 tunnel destination 192.168.10.219
 tunnel protection ipsec profile IKEV2-RA-PROFILE
 no tunnel protection ipsec initiate
end
```

show crypto ipsec sa peer <AnyConnect Public IP >(으)로 AnyConnect 클라이언트에 대한 IPsec SA(보안 연결)**를 확인합니다**.

```
cEdge-207#show crypto ipsec sa peer 192.168.10.219
interface: Virtual-Access2
   Crypto map tag: Virtual-Access2-head-0, local addr 192.168.10.218
  protected vrf: 1
  local  ident (addr/mask/prot/port): (0.0.0.0/0.0.0.0/0/0)
  remote ident (addr/mask/prot/port): (10.20.14.13/255.255.255.255/0/0)
  current_peer 192.168.10.219 port 50787
    PERMIT, flags={origin_is_acl,}
   #pkts encaps: 0, #pkts encrypt: 0, #pkts digest: 0
   #pkts decaps: 0, #pkts decrypt: 0, #pkts verify: 0
   #pkts compressed: 0, #pkts decompressed: 0
   #pkts not compressed: 0, #pkts compr. failed: 0
   #pkts not decompressed: 0, #pkts decompress failed: 0
   #send errors 0, #recv errors 0
    outbound pcp sas:
… Output Omitted….
```

세션, 사용자 이름 및 할당된 IP에 대해 IKEv2 SA 매개변수를 확인합니다.

참고: 할당된 IP 주소는 AnyConnect Client 측의 IP 주소와 일치해야 합니다.

```
cEdge-207#sh crypto ikev2 session detail
 IPv4 Crypto IKEv2 Session
Session-id:21, Status:UP-ACTIVE, IKE count:1, CHILD count:1
Tunnel-id Local                 Remote                fvrf/ivrf            Status
1         192.168.10.218/4500   192.168.10.219/62654  none/1               READY
     Encr: AES-CBC, keysize: 256, PRF: SHA256, Hash: SHA256, DH Grp:19, Auth sign: RSA, Auth
verify: AnyConnect-EAP
     Life/Active Time: 86400/532 sec
     CE id: 1090, Session-id: 21
     Local spi: DDB03CE8B791DCF7       Remote spi: 60052513A60C622B
     Status Description: Negotiation done
     Local id: 192.168.10.218
     Remote id: *$AnyConnectClient$*
     Remote EAP id: anavazar@cisco.com
     Local req msg id:  0              Remote req msg id:  23
     Local next msg id: 0              Remote next msg id: 23
     Local req queued:  0              Remote req queued:  23
     Local window:      5              Remote window:      1
     DPD configured for 45 seconds, retry 2
     Fragmentation not  configured.
     Dynamic Route Update: disabled
     Extended Authentication not configured.
     NAT-T is detected  outside
     Cisco Trust Security SGT is disabl
      Assigned host addr: 10.20.14.19
     Initiator of SA : No
Child sa: local selector  0.0.0.0/0 - 255.255.255.255/65535
          remote selector 10.20.14.19/0 - 10.20.14.19/65535
         ESP spi in/out: 0x43FD5AD3/0xC8349D4F
         AH spi in/out: 0x0/0x0
         CPI in/out: 0x0/0x0
         Encr: AES-CBC, keysize: 256, esp_hmac: SHA96
```

```
        ah_hmac: None, comp: IPCOMP_NONE, mode tunnel
 IPv6 Crypto IKEv2 Session

cEdge-207#show crypto session detail
Crypto session current status
Code: C - IKE Configuration mode, D - Dead Peer Detection
K - Keepalives, N - NAT-traversal, T - cTCP encapsulation
X - IKE Extended Authentication, F - IKE Fragmentation
R - IKE Auto Reconnect, U - IKE Dynamic Route Update
S - SIP VPN
Interface: Virtual-Access1
Profile: RA-SDWAN-IKEV2-PROFILE
Uptime: 00:17:07
Session status: UP-ACTIVE
Peer: 192.168.10.219 port 62654 fvrf: (none) ivrf: 1
     Phase1_id: *$AnyConnectClient$*
     Desc: (none)
 Session ID: 94
 IKEv2 SA: local 192.168.10.218/4500 remote 192.168.10.219/62654 Active
         Capabilities:DN connid:1 lifetime:23:42:53
 IPSEC FLOW: permit ip 0.0.0.0/0.0.0.0 host 10.20.14.19
       Active SAs: 2, origin: crypto map
       Inbound:  #pkts dec'ed 89 drop 0 life (KB/Sec) 4607976/2573
       Outbound: #pkts enc'ed 0 drop 0 life (KB/Sec) 4608000/2573
```

관련 정보

- Cisco SD-WAN 원격 액세스
- FlexVPN 서버 구성
- AnyConnect 다운로드
- 기술 지원 및 문서 – Cisco Systems